OCPP Certification Program

Document 2

OCPP 1.6

Test Procedure & Test Plans

2026-07-09

V2.4.1

Contents

1. Introduction 4
2. Terms and definitions 4
3. References 5
4. Test overview 5
4.1 Test coverage 5
4.2 Test prerequisites 5
5. Test procedure and Responsibilities 7
5.1 Certification Documents & Support 7
5.2 Test Instrumentation & Test Plan 7
5.3 Test Procedures 7
5.4 Pass Criteria 7
5.5 Retesting 7
5.6 Issue handling 8
6. Test Setup 9
6.1 General setup 9
6.2 Charging Station Software Stack 11
6.3 Test setup for re-certification 12
6.4 Test laboratory tools 13
7. Conformance test plan 13
7.1 Introduction 13
7.1.1 Objective 13
7.1.2 Scope of tests 13
7.1.3 Acceptant and acceptance criteria 14
7.1.4 Optional functionalities within feature profiles 14
8. Conformance tests 14
8.1.1 Test basis for OCPP 1.6 14
8.1.2 Test approach 14
8.2 Test script certification run 15
8.3 Vendor Declaration of Conformance 16
9. Performance measurements 17
9.1 Introduction 17
9.1.1 Objective 17
9.1.2 Scope of tests 17
9.1.3 Acceptant and acceptance criteria 17

9.2 Performance measurements 17
9.2.1 Test basis 17
9.2.2 Test approach 18
9.2.3 Intake DUT 19
9.2.4 Entry and exit criteria 19
9.3 Test script 19
9.4 Performance measurement for OCPP Product Family 20
Appendix A: Protocol Implementation Conformance Statement 21
A.1 PICS OCPP 1.6 certificate 25
A.2 PICS for OCPP 1.6 performance measurement 29
Appendix B: Test tools 30
Appendix C: List of conformance tests 32
OCPP 1.6 (Full & Subset) 32
Appendix D: Conformance tests - OCTT Test Rules 43
Appendix E: Example EVs to use for testing 43

1. Introduction

This document describes the test procedure and the test plans of the OCPP Certification Program for OCPP 1.6.

The test procedure covers testing of:

- a Charging Station (incl. product subtypes)
- a Charging Station Management System (CSMS)
-

2. Terms and definitions

Term / abbreviation	Definition / description
Certification Profile	A set of OCPP functionalities developed by the OCA to target the needs of a specific business driver accredited by the Alliance.
Charging Station	Refers to a Charge Point (OCPP 1.6 terminology) or Charging Station (OCPP 2.0 terminology)
Charging Station software stack	A Charging Station software stack in this document is defined as software that: - supports OCPP communication - is run and tested separately, without being in a physical Charging Station - can show all required behavior of a Charging Station supporting OCPP as specified in the OCPP specification (for example: executing (virtual) charging transactions, combining Charging Profiles in a composite schedule, not allowing charging on unavailable connectors etc.).
CSMS	Central System (OCPP1.6 terminology) or Charging Station Management System (OCPP2.0 terminology)
Device	An OCPP based device eligible for OCPP certification. In this document, this refers to a Central System or a Charge Point.
DUT	Device Under Test: The device submitted by the vendor for OCPP certification.
OCA	Open Charge Alliance
Participants	Any company involved in the OCPP certification program.
PICS	Protocol Implementation Conformance Statement. The completed PICS document is provided by the vendor to the Test Laboratory, asserting which OCPP specific requirements are met by its device.
Test Laboratory	An independent test laboratory authorized by the Open Charge Alliance to administer the approved OCPP tests and to assess eligibility of devices for OCPP certification.
Vendor	A manufacturer (OEM) of a Charging Stations or developer of a CSMS or Charging Station Software Stack, submitting devices for certification.

3. References

No	Title
1	OCPP Certification Procedure

4. Test overview

4.1 Test coverage

To become OCPP certified, the tested Device Under Test (DUT), has to successfully pass the following parts:

- **Conformance tests:** the tested DUT is tested against the OCPP Compliance Testing Tool. The tool has built in validations that should not fail during certification tests. With these validations the Tool verifies whether the DUT has implemented the OCPP specification correctly. The optional features of the OCPP protocol are also covered by the certification, if supported by the DUT. The set of optional features is listed in appendix C.
- **Performance measurements:** a number of performance values of the tested DUT are measured and give an idea how the device behaves in a lab environment. The performance parameters are stated by the vendor in the Protocol Implementation Conformance Statement (PICS).

4.2 Test prerequisites

The following prerequisites are applicable for certification testing:

- A Protocol Implementation Conformance Statement (PICS) has to be completed by the vendor of a DUT when submitting a solution for OCPP certification (See

- Appendix A: Protocol Implementation Conformance Statement). This should include all relevant limits and non-OCPP settings that are relevant for the test laboratory and for the correct functioning of the Charging Station / CSMS.
- When starting the certification process of an OCPP Product Family, all family members must be added to the PICS so that the test lab can choose a representative product.
- As a part of the certification process, the test lab will verify the PICS and in case of a Charging Station, all configuration keys will be read, validated where applicable and added to the test report.
- For CSMS:
    - The vendor shall supply either a running copy of a CSMS on a server / laptop to the test laboratory or give the test laboratory access to a running copy of the CSMS on a separate environment that is accessible via the Internet (e.g. a cloud environment). In the latter case, an Internet connection from the test laboratory to the CSMS shall be made available. This environment shall be "handed over" to the test laboratory and not updated by the vendor without knowledge of the test laboratory.
- For Charging Station:
    - A network connection to the Charging Station should be available via a telecom connection or wired ethernet connection.
    - To be able to test actual transactions, an EV is needed or has to be simulated. In the current EV market multiple types of sockets exist and no affordable EV simulators for all types of sockets are available at the time of writing. If an EVSE tester is available, this can be used (e.g. a type 2 socket to regular household socket with a dummy device (e.g. heater)). If no EV test socket or other test device is available at the testlab for a socket type, an EV is used. Testing a product subtype Mode 1/2-only Charging Station always requires using an EV instead of an EVSE tester. Please refer to Appendix E for examples of EVs that could be used per socket type.
- For a Charging Station software stack
    - The vendor must supply a software stack, running on a machine (this can be a laptop or a specific device running the software)
    - The vendor must implement a prescribed OCA API (that will be distributed separately) to trigger "manual" actions in the Charging Stations stack or a simple UI for triggering the functions (see 0).
- For both Charging Stations and Charging Station Software Stacks, the OCTT will determine which Firmware / OCPP Software Version is running during testing. This is done by reading the firmwareVersion field in the BootNotification field that must be implemented and filled by the vendor. The OCTT will automatically log the value.
- A technical representative of the Vendor is allowed to participate to the tests. If not physically present, a remote support from the technical team of the vendor *must* be arranged between the vendor and the test laboratory to help solving any issue raised during the certification tests.
- A Charging Station that supports more than 1 security profile, has to be delivered with the lowest supported security level. During certification it will be upgraded.
- To successfully execute the mandatory conformance test cases, the prerequisites for these tests have to be met.

5. Test procedure and Responsibilities

5.1 Certification Documents & Support

Test plans, configuration guides and engineering support are made available by the Test Laboratory to vendors in all stages of a vendor's preparation for certification. The responsibility for the test plans lies with the Open Charge Alliance.

5.2 Test Instrumentation & Test Plan

The Test Laboratory will distribute information to vendors regarding the test instruments that will be used during the certification tests if requested.

5.3 Test Procedures

Testers of the test laboratory will execute all tests and test procedures adhering strictly to the OCPP tests plans. Engineering staff from vendor companies may be present. Their presence may be required to resolve issues that may arise in the course of testing.

5.4 Pass Criteria

To be certified a vendor must successfully pass all tests described in chapter 4 and as defined in the OCPP test plans for the CSMS or Charging Station submitted for certification.

In exceptional cases (e.g. in case of bugs in OCPP Compliance Testing Tool) the OCA Compliance Working group can decide that a vendor is certified despite not passing all tests according to the test plans.

5.5 Retesting

Testers of the test laboratory will execute all tests and test procedures that are applicable for the Protocol Implementation Conformance Statement (PICS) that is reported by the vendor prior to the certification. If one or more tests fail, this will be reported back to the vendor and no certificate will be awarded (yet).

The policy for re-testing for the certification testing by the test laboratories is described below.

- Certificates are only valid for the device tested by the test laboratories and apply for a specific hardware feature set and a specific Firmware / OCPP software version;
- Any change on the device (hardware feature set or Firmware / OCPP software version) during the course of testing is not allowed and will require a full re-test of the DUT by the test laboratory;

- If a device “crashes” and requires a reset during conformance testing, this is considered as failing the conformance tests (and thus certification) and will thus require a re-test of the certification laboratory. This excludes crashes or problems caused by improper handling of the device by the test laboratory.

In case of un-clarity regarding the re-testing procedure, only the CWG of the Open Charge Alliance is authorized to decide on the procedure to be followed and this is not to be discussed between the Test Laboratory and the vendor.

5.6 Issue handling

Handling issues during tests can be separated in the following types:

- Configuration / setup issues. These are solved during testing, if necessary with the help of the technical representative of the vendor. When during the testing of a device a non-OCPP configuration is changed, all certification tests should be started over again;
- Bugs in software / hardware. This is considered as failing the certifications tests. See also 5.5 for handling of this situation.

6. Test Setup

6.1 General setup

The test setup used for Conformance testing is similar to the setup for the performance measurements. In order to have a fair comparison the connection properties are measured as part of the test. The test setups for testing are displayed in Figure 1 to Figure 3.

In Figure 1 the setup for a CSMS with a fixed ethernet connection is displayed. The CSMS is connected to the internet as well as the machine running the OCPP Compliance Testing Tool. Before starting the actual tests, the bandwidth as well as the latency for the network connection are measured. Please refer to the next paragraph for more information on the Test laboratory connection tester.

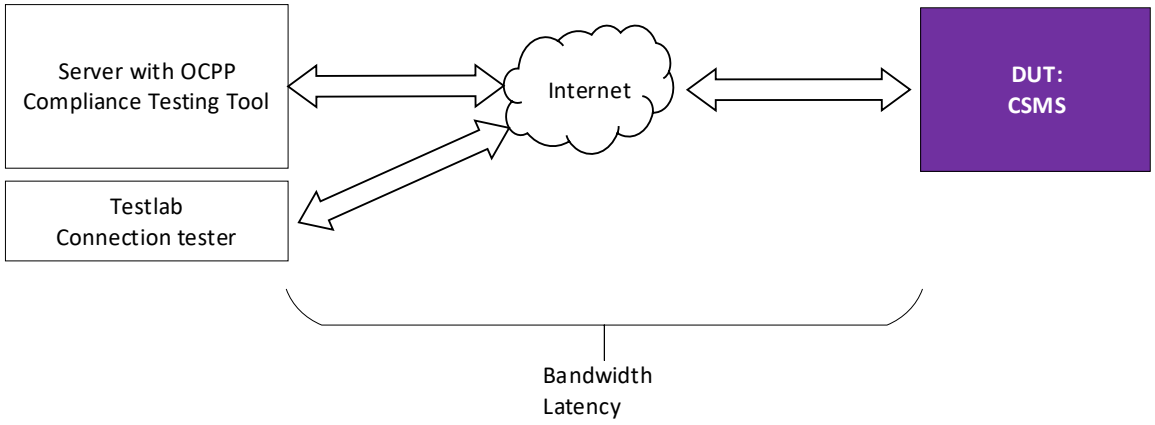

Figure 1: CSMS with fixed ethernet connection

In Figure 2 the setup for Charging Stations with a fixed ethernet connection or WiFi connection are displayed. In case of a fixed ethernet connection the Charging Station is connected via a UTP cable to a router that is connected to the internet. To be able to test actual transactions, actual EVs, EV test sockets or other test devices are used. In the current EV market multiple types of sockets exist and no affordable EV simulators for all types of sockets are available at the time of writing. For this reason, if no EV test socket or other test device is available at the testlab, an EV is to be used (e.g. rented). Testing a product subtype Mode 1/2-only Charging Station always requires using an EV instead of an EVSE tester. In case of Mode 2 charging, an in-cable control- and protection device, i.e. an IEC 61851 PWM controller, is used to connect the Charging Station to the EV. Please refer to Appendix E for examples of EVs to use per socket type.

For both ethernet and WiFi connections, a limited access router is included in the setup. This is for enforcing a direct connection to the OCPP Compliance Test Tool, as it is required for an OCPP Charging Station to speak OCPP directly, not – for example – via a cloud server.

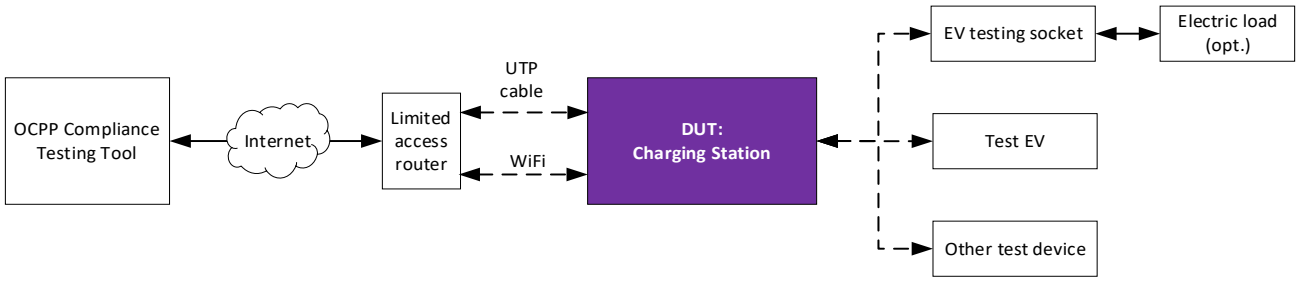

Figure 2: Charging Station with fixed ethernet connection

In Figure 3 the setup for a Charging Station with a telecom-only connection is displayed. The Charging Station is connected via mobile network to the OCPP Compliance Testing Tool. To be able to test bandwidth, 2 SIM cards (same network operator) are used: 1 for the Charging Station under test and 1 for testing the mobile internet connection at that location, with a Testlab Connection tester. The SIM cards will be provided by the test labs.

To be able to test actual transaction, test sockets / test devices are used (see explanation above).

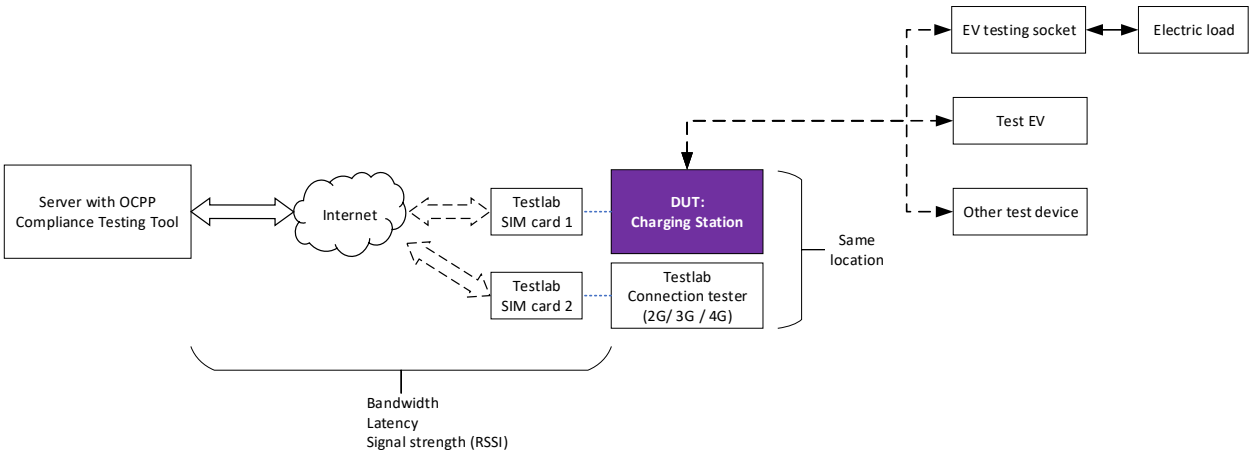

Figure 3: Charging Station with (only) telecom connection

For the tests where the DUT is a Charging Station, the OCA will provide test RFID cards that can be used in combination with the OCPP Compliance Testing Tool.

6.2 Charging Station Software Stack

In Figure 4 the test setup for a Charging Station software stack is displayed. If only the software stack is tested, parts of the Charging Station must be available in simulated / emulated form to enable the test laboratory tester to perform a full certification test. It is up to the vendor to provide a running copy (e.g. on a laptop, in cloud), the only requirement is that it is possible to setup a network connection to OCPP Compliance Testing Tool. This should be available via a telecom connection, WiFi or wired ethernet connection.

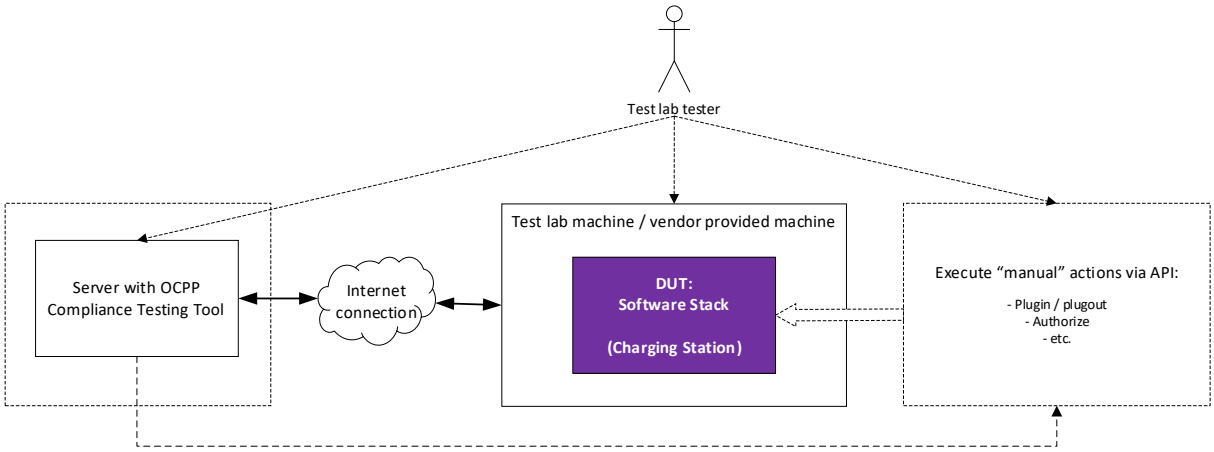

Figure 4: Test setup for testing Charging Station software stacks

In this test setup, the tester from the test laboratory will control the OCPP Compliance Testing Tool, but must also be enabled *by the vendor* to perform the manual actions that would be needed to control a physical Charging Station *using an OCA prescribed API*. This is the API belonging to the OCTT for OCPP 1.6 that will be distributed separately when applying for certification[1]. This means that a vendor must provide this API implementation to allow the test laboratory tester to perform the following actions:

- Plugin / plugout for all (virtual) connectors
- (De)authorize (e.g. simulate swiping an RFID card). When simulating RFID card swiping, it should be possible to use at least 2 different idTokens.
- Suspending charging on EV & EVSE side
- Cold booting a Charging Station (only restarting the software stack suffices)

In addition, the following rules specifically apply for a Charging Station Software Stack:

- During a charging session, the DUT must also be able to send Metervalues.

[1] only in exceptional cases, if approved by OCA and if the test lab agrees, an alternative can be used.

- Resetting: the rebooting / reconnection as defined in the requirements must be triggered by the OCPP implementation (i.e. the stack must initiate this). In this case there are 2 options for the reset:
    - Rebooting is done automatically by the software stack restarting itself.
    - Rebooting can be done manually by the test lab tester, but only by a clear notification of the implementation (-> not the OCPP message, but the message to the hardware or a simple UI).
- Updating firmware: the software stack must be able to go through all OCPP specified steps that are part of a firmware update, including the download, notifications, described security validations (e.g. firmware signing certificate and signature check) and reboot / reconnect.
- Uploading charger logs: a software stack must be able to go through all OCPP specified steps that are part of uploading logfiles. It is not required that logfiles contain hardware related information.

It is the responsibility of the vendor to provide a running setup of the stack (including the API) at the testing laboratory location.

6.3 Test setup for re-certification

When re-certifying it is allowed – but not required - to use the API, to save time for the manual actions on a DUT by the test lab. The test setup-for a Charging Station and CSMS when re-certifying an implementation is similar to the general test setup described in 6.1. However, the manual actions that are performed in the DUT are now done via the API of the OCTT to the DUT. For Charging Stations, a vendor must provide the OCTT API implementation to allow the test laboratory tester to perform the following actions:

- Plugin / plugout for all (virtual) connectors
- (De)authorize (e.g. simulate swiping an RFID card). When simulating RFID card swiping, it should be possible to use at least 2 different idTokens.
- Suspending charging on EV & EVSE side

For CSMS a separate OCTT API is available that triggers messages from a CSMS towards the Charging Station that are required by the test cases.

6.4 Test laboratory tools

The Test laboratory will use the following test tools:

- EVSE tester plug for AC type 1
- EVSE tester plug for AC type 2
- EV simulator / test socket for DC charging (tbd)
- Mobile communication dongle that supports enabling and disabling 2G, 3G and 4G
- OCPP Compliance Testing Tool (OCTT)
- Test laboratory connection tester

Test laboratory connection tester

The test laboratory shall use a “connection tester”, which refers to hardware / software that can measure:

- the internet connection from the server with OCPP Compliance Testing Tool to the CSMS under test. This will be done by executing an online internet speed test on both the CSMS as well as the machine running the OCPP Compliance Testing Tool.
- the properties of the internet connection (2G and / or 3G and / or 4G) from the server with OCPP Compliance Testing Tool to the location of the Charging Station under test.
  This can for example be done by using a mobile communication dongle and a laptop. This dongle must support enabling and disabling 2G, 3G and 4G. For each type, an online internet speed test will be executed, to determine the bandwidth / latency. For determining the signal strength, separate software could in this setup be used to determine the signal strength (actual results depends on the dongle used, but it is merely to get an indication of the signal strength).
  For uniformity, the same device is to be used for this by all labs. Please refer to Appendix B for the exact device that will be used.

7. Conformance test plan

7.1 Introduction

This chapter describes the conformance test plan for vendors to successfully complete as part of the OCPP certification program.

7.1.1 Objective

The objective of the conformance tests is to verify and validate the correct implementation of the OCPP protocol of a Charging Station or CSMS.

7.1.2 Scope of tests

The scope of the conformance tests is to verify and validate the correct implementation of the OCPP protocol of a Charging Station or CSMS by testing the DUT against the OCPP Compliance Testing Tool (OCTT) which automatically validates the responses by the DUT. Furthermore, the basic functionalities that are a consequence of messages in the OCPP protocol of a Charging Station or CSMS are verified and validated during these OCTT tests.

These tests are done by doing manual checks while running scenarios from the OCPP Compliance Testing Tool.

7.1.3 Acceptant and acceptance criteria

The Test Laboratory that executes the conformance test is not responsible for accepting or rejecting an OCPP implementation, but only responsible for executing the conformance test and reporting the results to the vendor and OCA.

The acceptance criteria for the conformance test is that all mandatory and applicable conditional tests for certification are executed successfully.

7.1.4 Optional functionalities within feature profiles

OCPP holds some optional Charging Station functionalities within the enclosed environment of a feature profile. These functionalities are managed by Read-only / Optional Configuration Keys. A issued certificate contains the following information:

- Whether the optional configuration keys are implemented or not.
- What value the implemented “Read-only” configuration keys contain.
- Description of the functionalities belonging to the configuration keys.

8. Conformance tests

8.1.1 Test basis for OCPP 1.6

The basis for testing conformance is the OCPP 1.6 edition 2 specification (date: 2017-09-28), OCPP 1.6 Errata sheet v4.0 Release (date: 2019-10-23) and OCPP 1.6 security whitepaper edition 3 (date: 2022-02-17)

Additionally, the following documentation is used:

- the scenarios for conformance testing are documented in Appendix C: List of conformance tests. This list contains the list of mandatory and conditional scenarios from the OCPP Compliance Testing Tool.

8.1.2 Test approach

The approach of testing is to test the DUT using the OCPP Compliance Testing Tool, manual functional verifications are executed during these conformance tests. Between tests, a utility test case (000_RESET) from the OCPP Compliance Testing Tool is used (and must pass) to set the Charging Station to a basic idle state to prevent test cases influencing each other.

The overall test process consists of the following steps:

- The Internet connection properties are measured.
- Test scenarios are started automatically using the OCPP Compliance Testing Tool.
- Most messages are automatically exchanged.
- Manual actions are executed by a test laboratory tester.

- Manual / on screen validations are executed by a test laboratory tester.

Intake DUT
As part of the conformance test, the following intake is done:

- A short pre-test is done to show that the DUT is functioning and is not, for example, damaged during transport.
- As an input the vendor should indicate whether or not the DUT supports sending milliseconds in OCPP messages.

Entry and exit criteria
Entry criteria for executing conformance test:

- All prerequisites that are documented in the OCPP Certification Procedure shall be met.
- All prerequisites that are documented in the OCPP Certification Test Procedure shall be met.
- Sufficient documentation about the DUT is available to the test laboratory in order to execute the manual actions for the test scenarios.

Exit criteria for executing conformance test:

- All mandatory test scenarios from Appendix C shall be executed successfully.

8.2 Test script certification run

The actions that are executed for the conformance tests are the following:

Preparation:

1. A running instance of the OCPP Compliancy Testing Tool is provided to the test laboratory (once)
2. The OCPP Compliancy Testing Tool UI is opened in a browser
3. The tester chooses the system that is tested
4. The information from the PICS is uploaded in the OCTT
5. The remaining configuration is entered in the OCTT
6. The test configuration is (automatically) added to the “OCPP Certification Report”.

Execution will be done for each test. The list of test cases that needs to be performed based on the PICS, is pre-filtered by the OCTT for the test lab and presented randomized by the OCTT. For each test case the following steps are performed:

1. If testing a Charging Station:
    a. The charging station is returned to basic state of operations using the OCTT restore mechanism (must be executed *successfully* before continuing)

2. If a transaction is running, the OCTT attempts to stop the transaction.
3. The test case is started in the OCTT. The Id and name used in the test tool user interface can be found in Appendix C and the separate OCPP 1.6 Test Cases document for more details and, if applicable, the conditions for this test case.
4. The steps in the scenario details in the OCPP 1.6 Test Cases document and the instructions given by the tool user interface are followed. Tool validations are done automatically.
5. After finishing the test case in the OCTT: based on the outcome of the test (PASS / FAIL / INCONC) and the OCTT test rules (see Appendix B), the result of the scenario is determined.

The Test Report is updated accordingly and can be exported after the certification run. A test report is generated including the OCTT configuration used and – for charging stations only - a hash of the firmware that was installed during test case TC_044_1_CS. This hash will also be printed on the OCPP Certificate. Please note that the image provided by the vendor to the test lab therefore must be a full image of the firmware for allowing an initial install (without any dependencies).

8.3 Vendor Declaration of Conformance

When a vendor wants to create a Vendor Declaration of Conformance for a product that is part of a product family, the following steps must be followed:

1. The PICS must be filled in correctly (please note: this cannot be changed during a run!)
2. The PICS must be loaded in the OCTT which means that it automatically selects the certification profiles, applicable test cases and configuration for the Charging Station
3. The OCTT will automatically run all test cases in PICS mode. All test cases must be run automatically, without human intervention, within 1 day, without interruptions.
4. Some test cases are (automatically) run multiple times, e.g. the test cases related to the authorization options.
5. If all test cases are passed, the OCTT will generate a Vendor Declaration of Conformance Report, which is digitally signed by OCTT.

9. Performance measurements

9.1 Introduction

This chapter describes the performance measurements that are performed by the test laboratory as part of the OCPP certification program.

9.1.1 Objective

The objectives of the Performance measurements are to measure the performance of a DUT within a lab context and to provide these as additional information to the certificate. The purpose of the Performance measurement is to measure the performance parameters that are stated by a vendor in the Protocol Implementation Conformance Statement (PICS).

9.1.2 Scope of tests

The scope of the performance measurement is to measure a number of performance parameters that are stated by a vendor in the Protocol Implementation Conformance Statement (PICS). For the example template for a PICS related to performance, please refer to Appendix A.4. The values that are stated by the vendor in the PICS do not have to fall within a set of upper / lower boundaries for certification, but will only be included in the test report to provide information to buyers of a device. These performance parameters are listed in paragraph 9.2.1.

9.1.3 Acceptant and acceptance criteria

The Test Laboratory that executes the performance measurement is not responsible for accepting or rejecting an OCPP implementation, but only responsible for executing the performance measurement and reporting the results to the vendor and OCA.

The only acceptance criterium for the performance measurement is that all parameters from the PICS are measured.

9.2 Performance measurements

9.2.1 Test basis

OCPP 1.6

The basis for the measurements is the OCPP 1.6 edition 2 specification (date: 2017-09-28), OCPP 1.6 Errata sheet v4.0 Release (date: 2019-10-23) and OCPP 1.6 security whitepaper edition 3 (date: 2022-02-17).

The following list of performance parameters is used:

Name	Description
OCPP triggered function timeout	The timeout used for when waiting for an OCPP function with its corresponding request message (e.g. time between receiving ChangeAvailability.conf and StatusNotification.req). Messages to the DUT can be handled within this timeout. This value excludes firmware, diagnostics and rebooting (e.g. based on a reset)
OCPP response timeout	The timeout used for when waiting for an OCPP response message. Messages to the DUT can be handled within this timeout.
Response time Authorize	The response time for the Authorize message.
Transaction authorization time by RemoteStartTransaction	The time between the RemoteStartTransaction.req message and the corresponding StartTransaction.req. Only cases where the RemoteStartTransaction immediately results in an authorization followed by a StartTransaction.req are included.
Transaction authorization end time by RemoteStopTransaction	The time between the RemoteStopTransaction.req message and the corresponding StopTransaction.req. Only cases where the RemoteStopTransaction immediately results in an end of the authorization followed by a StopTransaction.req are included.

9.2.2 Test approach

Performance measurements will be done in the following way: for measuring message timeouts the OCPP Compliance Testing Tool for OCPP is used. This tool logs all messaging. Based on this logging, the response times are determined.

As introduced in chapter 6, the tests are executed in a predefined test setup. Especially for performance measurements, this setup is important to get accurate measurements. Furthermore; it is important to measure performance in detail, without including effects that are out of control of a DUT.

In case of the OCPP protocol the main bottleneck is the network connection between the Charging Station and the CSMS. For this reason a number of parameters related to bandwidth is measured in (and by) the test laboratory before and during the measurement when a mobile connection is used. This is done using a mobile communication dongle connected to a laptop at the same location. This is (of course) only an indication to make sure that the mobile communication network is available at that location.

The following table lists the parameters that are measured concerning the network connection:

Parameter	Unit	Minimum / maximum for test setup*
Bandwidth	kB per second	Minimum: 5 kB per second
Latency	ms	Maximum: 1000 ms
Signal strength (RSSI) if applicable	dBm	Minimum: -81 dBm (CSQ 16)

* If these values are not met, the test lab should change the setup to improve the connection, before executing the measurement.

Please note: only 1 communication technology is measured for performance, so if multiple technologies available in a Charging Station, the technology that has to be used for the measurements must be stated in the PICS for performance.

9.2.3 Intake DUT

As part of the performance measurement, the following intake is done:

- Connectivity between the OCPP Compliance Testing Tool to the DUT is setup and measured (bandwidth, latency, RSSI).
- If not done during previous tests, a short pre-test is done to show that the DUT is functioning and is not, for example, damaged during transport.

9.2.4 Entry and exit criteria

Entry criteria for executing performance measurements:

- All prerequisites that are documented in the OCPP Certification Procedure shall be met.
- All prerequisites that are documented in the OCPP Certification Test Procedure shall be met.
- Sufficient documentation about the DUT is available to the test laboratory in order to execute the manual actions for the test scenarios.

Exit criteria for executing performance measurements:

- All performance criteria that are listed in 9.2.1 shall be measured.

9.3 Test script

The actions that are executed for the performance measurements are the following:

Preparation for a Charging Station:

1. The Charging Station that is tested, must be configured in the OCPP Compliance Testing Tool.
2. The network parameters as described in paragraph 9.2.2 are measured. In case of a poor network connection, it is attempted to optimize the connection so that it does not influence the performance measurements results.

Preparation for a CSMS:

1. The CSMS must be configured in the OCPP Compliance Testing Tool.
2. The network parameters as described in paragraph 9.2.2 are measured. In case of a poor network connection, it is attempted to optimize the connection so that it does not influence the performance measurements results.

For the timeout values, the OCPP Compliance Testing Tool logs are used to determine the measured values. The Test Report is updated accordingly.

9.4 Performance measurement for OCPP Product Family

When a vendor certifies for multiple products that belong to an OCPP product family, only the Representative Product for the OCPP family will be completely tested including a performance measurement by an OCA Designated test laboratory. The other OCPP family members will be added by validating a Vendor Declaration of Conformance. The performance measurement of the family members are *not* part of the Vendor Declaration of Conformance and thus not added to the certificate.

Appendix A: Protocol Implementation Conformance Statement

There are three PICS:

1. PICS for OCPP1.6
2. PICS for OCPP1.6 Security
3. PICS for OCPP1.6 Performance Measurement

General information about DUT

The following table should list the general information about the DUT:

Vendor name	<>
DUT	CSMS / Charging Station / Charging Station Software Stack
Product subtype	N.A. / Mode 1/2-only Charging Station
Type / model (for CS only)	<type name and / or model number>
Socket(s) / connector(s) (for CS only)	Singe / multiple
Fixed cable (for CS only)	<Yes / No>
Firmware / OCPP Software version	<version>
Support for milliseconds in OCPP messages	Yes / No
Communication technology	WiFi / ethernet / mobile network
RFID readers	none / single /one per EVSE

Optional features

The following table should list the presence / absence of some optional features:

	Feature	Supported / present
C-02	Support for allowing Offline Authorization for Unknown Ids (AllowOfflineTxForUnknownId)	*Yes / No*
C-03	Support for maximizing energy for invalid ids (*MaxEnergyOnInvalidId)*	*Yes / No*
C-04	Authorization Cache (AuthorizationCacheEnabled)	*Yes / No*
C-05	Support to limit StatusNotifications (MinimumStatusDuration)	*Yes / No* If supported by a Charging Station, the station is to be delivered to the test lab with the value set to 0.

C-06	Authorization status after cable disconnected on EV side (StopTransactionOnEVSideDisconnect)	Yes / No / Both
C-07	Support for local start	Yes / No
C-08	Support for local stop	Yes / No
C-10	Unlocking of connector when cable disconnected on EV side (UnlockConnectorOnEVSideDisconnect)	Yes / No / Configurable
C-11	Support for Security Profile 1	Yes / No
R-0	Support for Reservations	Yes / No
R-1	Support reservations of entire Charging Station (ReserveConnectorZeroSupported)	Yes / No
SC-1	Supported charging rate units (ChargingScheduleChargingRateUnit)	A / W / Both
LA-0	Support for Local Authorization List Management	Yes / No
RT-0	Support for Remote Trigger	Yes / No

Supported cipher suites (Charging Station only)[2]

Cipher suite	Supported
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 AND TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	Yes / No
TLS_RSA_WITH_AES_128_GCM_SHA256 AND TLS_RSA_WITH_AES_256_GCM_SHA384	Yes / No

Additional questions Charging Station:

Id	Additional questions for lab testing	Supported / present
AQ-1	Can the last CentralSystemRootCertificate can be removed?	*Yes / No*
AQ-2	Does the Charging Station have a cable lock, which prevents the EV driver to connect the EV and EVSE before authorization?	*Yes / No*
AQ-3	Can the last ChargePointCertificate be removed (via other means than OCPP)?	*Yes / No*
AQ-4	Is your Charging Station able to download firmware while there is an ongoing transaction?	*Yes / No*
AQ-5	Does your Charging Station enforce a selection of EVSE (by design) prior to authorization?	*Yes / No*

[2] Please note that the CSMS SHALL support at least the following four cipher suites: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_256_GCM_SHA384

AQ-6	Does your Charging Station support charging an EV using IEC 61851-1 (Mode 3)?	*Yes / No*
AQ-7	Reporting of StopTransaction after power loss	
AQ-7.1	Charge Point configured to report StopTransaction(s) before going down.	*Yes / No*
AQ-7.2	Charge Point configured to report StopTransaction(s) after going down and being back online again.	*Yes / No*
AQ-8	Does the Charge Point have additional communication ports besides the OCPP communication channel? *If so, please list these in the table on the right.*	*Yes / No*
AQ-9	Does your Charging Station have at least one connector with an (automatic) mechanized locking mechanism on Charging Station side? (this is always true for connectorTypes; sType2 and sType3)	*Yes / No*
AQ-11	Does your Charging Station support an authorization method, that does not rely on the communication between EV and Charging Station?	*Yes / No*

Additional questions CSMS:

Id	Additional questions for lab testing	Supported / present
AQ-10	Can your CSMS be configured to first respond to a BootNotificationRequest with status Pending or Rejected?	*Yes / No*

Other relevant settings and limits

The table below should contain all relevant limits and non-OCPP settings that are relevant for the test laboratory and for the correct functioning of the Charging Station / CSMS:

Limit / setting	Value
GetConfigurationMaxKeys	…
MeterValuesAlignedDataMaxLength	…
MeterValuesSampledDataMaxLength	…
Minimum MeterValueSampleInterval supported	…
Maximum MeterValueSampleInterval supported	…
Minimum HeartbeatInterval supported	…
Maximum HeartbeatInterval supported	…
StopTransactionMaxMeterValues	…
StopTxnAlignedDataMaxLength	…
StopTxnSampledDataMaxLength	…
WebSocketPingInterval	…
Local Authorization List	
LocalAuthListMaxLength	…
SendLocalListMaxLength	…

Smart charging	
ChargeProfileMaxStackLevel	**…**
ChargingScheduleMaxPeriods	**…**
Firmware Management	
Supported file transfer protocols	{http, https, ftp, ftps}
Other relevant values	
<other minimum value>	**…**
<other maximum value>	**…**
Security Extension	
CertificateSignedMaxChainSize	**…**
CertificateStoreMaxLength	**…**

IP configuration

The test laboratory will provide information on the network configuration that has to be configured on the Charging Station beforehand.

A.1 PICS OCPP 1.6 certificate

The Table below states the mandatory and optional functionalities for certification. When a functionality is supported by the DUT, all applicable use cases must be supported, unless stated otherwise.

Name	OCPP 1.6 Fully supported	OCPP 1.6 Subset supported	Description
Core	**Yes**	**Yes**	**Basic Charging Station functionality for booting, authorization (incl. cache if available), configuration, transactions, remote control.**
Included functionalities			
	Cold Boot Charge Point		
	Cold Boot Charge Point		
	Cold Boot Charge Point - Pending		
	Start Charging Session		
	Regular Charging Session - Plugin First		
	Regular Charging Session – Identification First		
	Regular Charging Session – Identification First - ConnectionTimeOut		
	Stop Charging Session		
	Stop transaction - IdTag in StopTransaction matches IdTag in StartTransaction		
	Stop transaction - ParentIdTag in StopTransaction matches ParentIdTag in StartTransaction		
	EV Side Disconnected		
	One Reader for Multiple Connectors		
	One Reader for Multiple Connectors (optional)		
	Cache (if available)		
	Regular Start Charging Session – Cached Id		
	Clear Authorization Data in Authorization Cache		
	Transaction Related Message not Accepted by Central System		
	Core Profile - Remote actions Happy Flow		
	Remote Start Charging Session – Cable Plugged in First		
	Remote Start Charging Session – Remote Start First		
	Remote Start Charging Session – connection timeout		
	Remote Stop Charging Session		
	Core Profile - Resetting Happy Flow		
	Hard Reset Without transaction		
	Soft Reset Without Transaction		
	Hard Reset With Transaction		
	Soft Reset With Transaction		

	Core Profile - Unlocking Happy Flow
	Unlock connector - no charging session running(Not fixed cable)
	Unlock connector - no charging session running(Fixed cable)
	Unlock Connector - With Charging Session
	Core Profile - Configuration Happy Flow
	Retrieve configuration (Charging Station only)
	Retrieve all configuration keys (CSMS only)
	Retrieve specific configuration key (CSMS only)
	Change/set Configuration
	Meter values
	Sampled Meter Values
	Clock-aligned Meter values
	Core Profile - Basic Actions Non-happy Flow
	Start Charging Session - Authorize invalid / blocked / expired
	Start Charging Session Lock Failure
	Send Local Authorization List - NotSupported
	Get Local List Version - NotSupported
	Core Profile - Remote Actions Non-Happy Flow
	Remote Start Charging Session - Rejected
	Remote Stop Transaction - Rejected
	Core Profile - Unlocking Non-happy Flow
	Unlock Connector - Unlock Failure
	Unlock Connector - Unknown Connector
	Core Profile - Power Failure Non-Happy Flow
	Power failure boot charging point-configured to stop transaction(s)
	Power Failure with Unavailable Status
	Core Profile - Offline behavior Non-Happy Flow
	Connection Loss During Transaction
	Offline Start Transaction
	Offline Stop Transaction
	Offline Transaction
	Core Profile - Configuration Keys Non-Happy Flow
	Configuration keys
	Diagnostics
	Get Diagnostics
	Get Diagnostics - Upload Failed
	Trigger Message
	Trigger Message - Rejected
	DataTransfer
	Data Transfer to a Charge Point
	Data Transfer to a Central System
	Security event/logging
	Get Security Log
	Secure firmware update
	Secure Firmware Update

	Secure Firmware Update - Invalid Signature		
	Update Charge Point Password for HTTP Basic Authentication		
	Install a certificate on the Charge Point		
	Delete a specific certificate from the Charge Point		
	Security Profile 1: Unsecured Transport with Basic Authentication		
	Secure connection setup		
	Security Profile 2: TLS with Basic Authentication		
	Secure connection setup		
Optional feature: Reservations	**Reservation of a Connector**		
	Reservation of a Connector – Local start transaction		
	Reservation of a Connector – Remote start transaction		
	Reservation of a Connector - Expire		
	Reservation of a Connector - Occupied		
	Reservation of a Connector - Unavailable		
	Reservation of a Connector - Rejected		
	Reservation of a Charge Point		
	Reservation of a Charge Point - Transaction		
	Reservation of a Charge Point - Occupied		
	Reservation of a Charge Point - Unavailable		
	Cancel Reservation		
	Cancel Reservation		
	Cancel Reservation - Rejected		
	Use a reserved Connector with parentIdTag		
Optional feature: Local Authorization List Management	**Get Local List Version**		
	Get Local List Version (empty)		
	Send Local Authorization List		
	Send Local Authorization List		
	Send Local Authorization List - VersionMismatch		
	Send Local Authorization List - Failed		
	Send Local Authorization List - Full		
	Send Local Authorization List - Differential		
	Regular Start Charging Session – Id in Local Authorization List		
Smart Charging	**Yes**	**Yes / No** (Not applicable for product subtype Mode 1/2-only Charging Station.)	**Support for Smart Charging (all profile types, including stacking), to control charging.**
Included functionalities			
	Central Smart Charging		

	Central Smart Charging - TxDefaultProfile		
	Central Smart Charging - TxProfile		
	Central Smart Charging - No ongoing transaction		
	Central Smart Charging - Wrong transactionId		
	Central Smart Charging - TxDefaultProfile - with ongoing transaction		
	Get Composite Schedule		
	Clear Charging Profile		
	Stacking Charging Profiles		
	Remote Start Transaction with Charging Profile		
	Remote Start Transaction with Charging Profile		
	Remote Start Transaction with Charging Profile - Rejected		
Advanced Security	**Yes**	**Yes / No**	**TLS (1.2 or higher) with Client Side Certificates**
Included functionalities			
	Security Profile 3: TLS with Client Side Certificates		
	Secure connection setup		

Update Charge Point Certificate by request of Central System

A.2 PICS for OCPP 1.6 performance measurement

Name	Value	Unit	Description
OCPP triggered function timeout (Charging Station only)	XX	seconds	The response time for when waiting for an OCPP function with its corresponding request message. (Firmware update, Diagnostics and Reboot are excluded from this measurement.) ***Message combinations checked:*** *CancelReservation / StatusNotification(status=Available)* *ReserveNow / StatusNotification(status=Reserved)* *ChangeAvailability / StatusNotification* *TriggerMessage / <Triggered Message>*
OCPP response timeout	XX	seconds	The response time for when waiting for an OCPP response message.
Response time Authorize (CSMS only)	XX	seconds	The response time for the Authorize message.
Transaction authorization time by RemoteStartTransaction (Charging Station only)	XX	seconds	The time between the RemoteStartTransaction.req message and the corresponding StartTransaction.req. Only cases where the RemoteStartTransaction immediately results in an authorization followed by a StartTransaction.req are included.
Transaction authorization end time by RemoteStopTransaction (Charging Station only)	XX	Seconds	The time between the RemoteStopTransaction.req message and the corresponding StopTransaction.req. Only cases where the RemoteStopTransaction immediately results in an end of the authorization followed by a StopTransaction.req are included.

The communication technology for which the measurements are done:

Communication technology	<WiFi / ethernet / mobile>

Please note: only 1 communication technology is measured for performance, so if multiple technologies availavle in a Charging Station, please select for which the measurements should be executed by the lab.

Appendix B: Test tools

The following tools are used during the certification tests:

- OCPP Compliance Testing Tool. This test tool is supplied to the Testing Laboratory and maintained by the Open Charge Alliance.
- Mobile communication dongle for performance measurements
    - Brand: Huawei
    - Type: E3372h LTE dongle
    - EV emulator for AC / DC Type 1/2 provided by OCA:
        - Brand / Type: Trialog / EVComboCS4M
    - Some labs use their own EV emulator for AC / DC Type 1/2, one of the following:
        - Brand / Type: Keysight / Charge Discovery system
        - Brand / Type: Comemso / EVCA-system

Appendix C: List of conformance tests

OCPP 1.6 (Full & Subset)

M = Mandatory

O = Optional

C = Conditional (condition in the “Remark” column)

	OCTT Id	OCPP Compliance Testing Tool scenario	Conf. Test for Charging Station	Conf. test for Central System	Remark
		CORE			
		Cold Boot Charge Point			
	TC_001	Cold Boot Charge Point	M	M	
	TC_002	Cold Boot Charge Point - Pending	M		
		Start Charging Session			
	TC_003	Regular Charging Session - Plugin First	C	M	Only applicable for a Charge Point which supports local start/stop transaction and does not have a cable lock (AQ-2).
	TC_004_1	Regular Charging Session – Identification First	C	M	Only applicable for a Charge Point which supports local start/stop transaction. AND the Charging Station supports an authorization method,

					that does not rely on the communication between EV and Charging Station (AQ-11)
	TC_004_2	Regular Charging Session – Identification First - ConnectionTimeOut	C	M	Only applicable for a Charge Point which supports local start transaction. AND the Charging Station supports an authorization method, that does not rely on the communication between EV and Charging Station (AQ-11)
		Stop Charging Session			
	TC_068	Stop transaction - IdTag in StopTransaction matches IdTag in StartTransaction	C		Only applicable for a Charge Point which supports local start/stop transaction.
	TC_069	Stop transaction - ParentIdTag in StopTransaction matches ParentIdTag in StartTransaction	C		Only applicable for a Charge Point which supports local start/stop transaction.
	TC_005_1	EV Side Disconnected - StopTransactionOnEVSideDisconnect = true - UnlockConnectorOnEVSideDisconnect = true	C	M	StopTransactionOnEVSideDisconnect = true, Condition: The Charge Point does not have a fixed cable on Charge Point side AND The configuration key StopTransactionOnEVSideDisconnect does NOT have the accessibility ReadOnly in combination with value false. AND UnlockConnectorOnEVSideDisconnect does NOT have the accessibility ReadOnly in combination with the value false. AND the Charging Station has at least one connector with an (automatic) mechanized locking mechanism on Charging Station side (AQ-9)
	TC_005_2	EV Side Disconnected - StopTransactionOnEVSideDisconnect = true - UnlockConnectorOnEVSideDisconnect = false	C		StopTransactionOnEVSideDisconnect = true, Condition:

					The configuration key StopTransactionOnEVSideDisconnect does NOT have the accessibility ReadOnly in combination with value false. AND UnlockConnectorOnEVSideDisconnect does NOT have the accessibility ReadOnly in combination with the value true. Mandatory for product subtype Mode 1/2-only Charging Station.
	TC_005_3	EV Side Disconnected - StopTransactionOnEVSideDisconnect = false - UnlockConnectorOnEVSideDisconnect = false	C		StopTransactionOnEVSideDisconnect = false, The configuration key UnlockConnectorOnEVSideDisconnect does NOT have the accessibility ReadOnly in combination with the value true. Not applicable for product subtype Mode 1/2-only Charging Station.
		Cache			
	TC_007	Regular Start Charging Session – Cached Id		M	
	TC_007_1	Regular Start Charging Session – Cached Id	C		Only applicable for a Charge Point which supports local start transaction AND if a cache is available.
	TC_007_2	Remote Start Charging Session – Cached Id	C		Applicable for a Charge Point which does NOT support local start transaction AND if a cache is available.
	TC_061	Clear Authorization Data in Authorization Cache		M	
	TC_061_1	Clear Authorization Data in Authorization Cache - Local	C		Only applicable for a Charge Point which supports local start transaction AND if a cache is available.
	TC_061_2	Clear Authorization Data in Authorization Cache - Remote	C		Applicable for a Charge Point which does NOT support local start transaction AND if a cache is available.
		Core Profile - Remote actions Happy flow			

	TC_010	Remote Start Charging Session – Cable Plugged in First	C	M	Only applicable for a Charge Point that does not have a cable lock (AQ-2)
	TC_011_1	Remote Start Charging Session – Remote Start First	M	M	
	TC_011_2	Remote Start Charging Session – Time Out	M	M	
	TC_012	Remote Stop Charging Session	M	M	
		Core Profile - Resetting Happy Flow			
	TC_013	Hard Reset Without transaction	M	M	
	TC_014	Soft Reset Without Transaction	M	M	
	TC_015	Hard Reset With Transaction	M		
	TC_016	Soft Reset With Transaction	M		
		Core Profile - Unlocking Happy flow			
	TC_017_1	Unlock connector - no charging session running (Not fixed cable)	C	M	Only applicable for a Charge Point with a detachable cable. AND the Charging Station has at least one connector with an (automatic) mechanized locking mechanism on Charging Station side (AQ-9)
	TC_017_2	Unlock connector - no charging session running (Fixed cable)	C	M	Only applicable for a Charge Point with a fixed cable. AND the Charging Station does NOT have at least one connector with an (automatic) mechanized locking mechanism on Charging Station side (NOT AQ-9)
	TC_018_1	Unlock Connector - With Charging Session (Not fixed cable)	C		Only applicable for a Charge Point with a detachable cable. AND the Charging Station has at least one connector with an (automatic) mechanized locking mechanism on Charging Station side (AQ-9)
	TC_018_2	Unlock Connector - With Charging Session (Fixed cable)	C		Only applicable for a Charge Point with a fixed cable. AND

					the Charging Station does NOT have at least one connector with an (automatic) mechanized locking mechanism on Charging Station side (NOT AQ-9)
		Core Profile - Configuration Happy flow			
	TC_019	Retrieve configuration	M		
	TC_019_1	Retrieve all configuration keys		M	
	TC_019_2	Retrieve specific configuration key		M	
	TC_021	Change/set Configuration	M	M	
		Meter values			
	TC_070	Sampled Meter Values	M		
	TC_071	Clock-aligned Meter Values	M		
		Core Profile - Basic Actions Non-happy flow			
	TC_023_1	Start Charging Session - Authorize invalid		M	
	TC_023_2	Start Charging Session - Authorize expired		M	
	TC_023_3	Start Charging Session - Authorize blocked		M	
	TC_023_4	Start local Charging Session - Authorize invalid	C		Only applicable for a Charge Point which supports local start transaction AND if a cache is available.
	TC_023_5	Start remote Charging Session - Authorize invalid	C		Applicable for a Charge Point which does NOT support local start transaction AND if a cache is available.
	TC_024	Start Charging Session - Lock Failure	O	M	Only applicable if the Charge Point does not have a fixed cable on Charge Point side.
	TC_043_1	Send Local Authorization List - NotSupported	C	O	If not supported by Charging Station.
	TC_042_1	Get Local List Version (not supported)	C	O	If not supported by Charging Station.
		Core Profile - Remote Actions Non-Happy Flow			
	TC_026	Remote Start Charging Session - Rejected	M	M	
	TC_028	Remote Stop Transaction - Rejected	M	O	
		Core Profile - Unlocking Non-happy flow			
	TC_030	Unlock Connector - Unlock Failure	O	M	

	TC_031	Unlock Connector – Unknown Connector	M	O	
		Core Profile - Power Failure Non-Happy Flow			
	TC_032_1	Power failure boot charging point - configured to stop transaction(s) before going down	C	M	Only applicable for a Charge Point configured to stop transaction(s) before going down.
	TC_032_2	Power failure boot charging point-configured to stop transaction(s)	C		Only applicable for a Charge Point configured to stop transaction(s) after going down and being back online again.
	TC_034	Power Failure with Unavailable Status	M		
		Core Profile - Offline behavior Non-Happy Flow			
	TC_036	Connection Loss During Transaction	M		
	TC_037_1	Offline Start Transaction - Valid IdTag	C	M	Only applicable for a Charge Point which supports local start/stop transaction and at least one of the following 3 functionalities: local authorization list feature profile, Unknown Offline Authorization or Authorization Cache. Using valid idTag, AllowOfflineTxForUnknownId = true, LocalAuthorizeOffline = true
	TC_037_2	Offline Start Transaction - Invalid IdTag - StopTransactionOnInvalidId = false	C		Only applicable for a Charge Point which supports local start/stop transaction and at least one of the following 3 functionalities: local authorization list feature profile, Unknown Offline Authorization or Authorization Cache. Using invalid idTag, AllowOfflineTxForUnknownId = true, LocalAuthorizeOffline = true, StopTransactionOnInvalidId = false Please note: as with all Charging Stations, this test case is also applicable for product subtype Mode 1/2-only Charging Station (depending on the above conditions).

	TC_037_3	Offline Start Transaction - Invalid IdTag - StopTransactionOnInvalidId = true	C	M	Only applicable for a Charge Point which supports local start/stop transaction and at least one of the following 3 functionalities: local authorization list feature profile, Unknown Offline Authorization or Authorization Cache. Using invalid idTag, AllowOfflineTxForUnknownId = true, LocalAuthorizeOffline = true, StopTransactionOnInvalidId = true
	TC_038	Offline Stop Transaction	C		Only applicable for a Charge Point which supports local stop transaction.
	TC_039	Offline Transaction	C	M	Only applicable for a Charge Point which supports local start/stop transaction and at least one of the following 3 functionalities: local authorization list feature profile, Unknown Offline Authorization or Authorization Cache.
		Core Profile - Configuration Keys Non-Happy Flow			
	TC_040_1	Configuration keys – NotSupported	M	O	Not supported configuration key.
	TC_040_2	Configuration Keys - Invalid value	M	O	Incorrect value.
		Diagnostics			
	TC_045_1	Get Diagnostics	M	M	For interop: check FTP connection
	TC_045_2	Get Diagnostics - Upload Failed	M	O	
		Remote Trigger			
	TC_054	Trigger Message	C	M	Only applicable if Remote Trigger supported
	TC_055	Trigger Message - Rejected	C	O	Only applicable if Remote Trigger supported
		Secure connection setup			
	TC_073	Update Charge Point Password for HTTP Basic Authentication	M	M	
	TC_075_1	Install a certificate on the Charge Point – ManufacturerRootCertificate	M	M	
	TC_075_2	Install a certificate on the Charge Point - CentralSystemRootCertificate	M	M	

	TC_076	Delete a specific certificate from the Charge Point	M	M	
		Security event/logging			
	TC_078	Invalid CentralSystemCertificate Security Event	M	M	
	TC_079	Get Security Log	M	M	
		Secure firmware update			
	TC_080	Secure Firmware Update	M	M	
	TC_081	Secure Firmware Update - Invalid Signature	M	M	
		Upgrade security profile			
	TC_083	Upgrade security profile	C	C	Only applicable if the DUT supports multiple security profiles
	TC_084	Downgrade security profile - Rejected	C		Only applicable if the DUT supports multiple security profiles
		Setup connection with security profiles			
	TC_085	Basic Authentication - Valid username/password combination	M	M	
	TC_086	TLS - server-side certificate - Valid certificate	M	M	
	TC_088	WebSocket Subprotocol negotiation		M	
		DataTransfer			
	TC_062	Data Transfer to a Charge Point	M		Only verifying that the DUT responds (rejecting is ok).
	TC_064	Data Transfer to a Central System		M	Only verifying that the DUT responds (rejecting is ok).
		Get Local List Version			
	TC_042_2	Get Local List Version (empty)	C	M	Only applicable if Local Auth. List supported
		Send Local Authorization List			
	TC_043	Send Local Authorization List	C		Only applicable if Local Auth. List supported Prerequisite: support for at least 5 idTokens is required.
	TC_043_2	Send Local Authorization List - VersionMismatch	C		Only applicable if Local Auth. List supported

	TC_043_3	Send Local Authorization List - Failed	O	M	
	TC_043_4	Send Local Authorization List - Full		M	
	TC_043_5	Send Local Authorization List - Differential		M	
	TC_008_1	Regular Start Charging Session – Id in Local Authorization List	C		Only applicable if Local Auth. List supported AND Only applicable for a Charge Point which supports local start transaction AND if a cache is available.
	TC_008_2	Remote Start Charging Session – Id in Local Authorization List	C		Only applicable if Local Auth. List supported Applicable for a Charge Point which does NOT support local start transaction AND if a cache is available.
		Reservation of a Connector			
	TC_046	Reservation of a Connector – Transaction		M	
	TC_046_1	Reservation of a Connector – Local start transaction	C		Only applicable if Reservations are supported. Only applicable for a Charge Point which supports local start transaction.
	TC_046_2	Reservation of a Connector – Remote start transaction	C		Only applicable if Reservations are supported
	TC_047	Reservation of a Connector - Expire	C	M	Only applicable if Reservations are supported
	TC_048_2	Reservation of a Connector - Occupied	C	O	Only applicable if Reservations are supported Only applicable for a Charge Point that does not have a cable lock (AQ-2)
	TC_048_3	Reservation of a Connector - Unavailable	C	O	Only applicable if Reservations are supported
	TC_048_4	Reservation of a Connector - Rejected	O	M	
		Reservation of a Charge Point			
	TC_049	Reservation of a Charge Point - Transaction	C	M	Only applicable if Reservations are supported Only applicable for a Charge Point which supports reserving an entire Charging Station.
	TC_050_2	Reservation of a Charge Point - Occupied	C		Only applicable if Reservations are supported

					Only applicable for a Charge Point which supports reserving an entire Charging Station and does not have a cable lock (AQ-2).
	TC_050_3	Reservation of a Charge Point - Unavailable	C		Only applicable if Reservations are supported Only applicable for a Charge Point which supports reserving an entire Charging Station.
		Cancel Reservation			
	TC_051	Cancel Reservation	C	M	Only applicable if Reservations are supported
	TC_052	Cancel Reservation - Rejected	C	O	Only applicable if Reservations are supported
	TC_053	Use a reserved Connector with parentIdTag		O	
	TC_053_1	Use a reserved Connector with parentIdTag - Local	C		Only applicable if Reservations are supported Only applicable for a Charge Point which supports local start transaction AND if a cache is available.
	TC_053_2	Use a reserved Connector with parentIdTag - Remote	C		Only applicable if Reservations are supported Applicable for a Charge Point which does NOT support local start transaction AND if a cache is available.
SmartCharging					
		Central Smart Charging			
	TC_056	Central Smart Charging - TxDefaultProfile	M	M	Not applicable for product subtype Mode 1/2-only Charging Station.
	TC_057	Central Smart Charging - TxProfile	M	M	Not applicable for product subtype Mode 1/2-only Charging Station.
	TC_058_1	Central Smart Charging - No ongoing transaction	M		Not applicable for product subtype Mode 1/2-only Charging Station.
	TC_058_2	Central Smart Charging - Wrong transactionId	M		Not applicable for product subtype Mode 1/2-only Charging Station.
	TC_082	Central Smart Charging - TxDefaultProfile - with ongoing transaction	M		Not applicable for product subtype Mode 1/2-only Charging Station.

	TC_066	Get Composite Schedule	M	M	Prerequisite: support for 3 installed profiles with 5 ChargingSchedule periods is required. Not applicable for product subtype Mode 1/2-only Charging Station.
	TC_067	Clear Charging Profile	M	M	Not applicable for product subtype Mode 1/2-only Charging Station.
	TC_072	Stacking Charging Profiles	M		Prerequisite: support for 2 stack levels is required. Not applicable for product subtype Mode 1/2-only Charging Station.
		Remote Start Transaction with Charging Profile			
	TC_059	Remote Start Transaction with Charging Profile	M	M	Not applicable for product subtype Mode 1/2-only Charging Station.
	TC_060	Remote Start Transaction with Charging Profile - Rejected	M		Not applicable for product subtype Mode 1/2-only Charging Station.
Advanced Security					
	TC_074	Update Charge Point Certificate by request of Central System	M	M	
	TC_077	Invalid ChargePointCertificate Security Event	M	M	
	TC_087	TLS - Client-side certificate - valid certificate	M	M	

Appendix D: Conformance tests - OCTT Test Rules

The following rules apply:

- For the Mode 1/2-only Charging Station, some devices use a slightly different flow than most stations. Although this flow is not advised, it is allowed during certification:
  - *Available* ->
  - Short power flow, status: *Preparing* ->
  - After power flow: status *Available* ->
  - After local authorization: status *Preparing* followed by status *Charging*.
- For the configuration of OCTT the following applies:
  - When validating/comparing time / dateTime values, the acceptable deviation is 4 seconds (OCTT: "Max time deviation" set to 4), except for metervalues. This is done to accommodate any discrepancies regarding internal clock synchronization, processing time, etc.
  - The acceptable deviation for metervalues is <1 second (OCTT: "Max Time Deviation for MeterValues" set to 1)
  - Because of the existence of the above deviation, other time-related configurations need to be configured with a value that is larger than the configured "Max time deviation". Therefore, the minimum set value for the configurations below needs to be > configured "Max time deviation" + 2 seconds. This applies to: Offline threshold, Transaction Duration, EV Connection Time Out (Sec), Heartbeat Interval, Upload diagnostics retry interval, Download Offset Period, Installation Offset Period, Expiry Date Offset.
- Currently no other rules are applicable.

Appendix E: Example EVs to use for testing

The following list contains example EVs that can be used for testing (non exhaustive):

Socket type	Possible EV (non-exhaustive list)
CHAdeMO	Citroën Berlingo Electric Citroën C-Zero Kia Soul EV Mitsubishi Outlander PHEV Nissan Leaf 2 or e-NV200
CCS	BWM i3 Hyundai Ioniq Hyundai KONA

	Kia e-Niro Opel Ampera-e Tesla Model 3 Volkswagen e-Golf or e-up
Tesla	Tesla model S / X